INFRASTRUCTURE ASSET MANAGEMENT: EVOLUTION AND INTEGRATION

BY RICH MCGUIRE, SR. PROCESS ENGINEER

Like many of readers of this publication, I frequently travel among my home, office, satellite facilities, and/or clients. I travel as a representative of Inframark, LLC, a contract operator, maintainer, and manager of municipal and industrial infrastructure and capital assets, including water and wastewater systems and underground utilities. Inframark utilizes cloud-based, enterprise data management systems to gather, store, and organize data generated by a wide array of equipment sensors, instrumentation, laboratory analyses, financial data bases, and human-machine interface (HMI). This data is sourced from facilities throughout the U.S. and used as a basis for decision-making at the local, regional, and corporate level. The current IT systems have a successful track record of supporting timely and accurate decision-making and, for the present time, provide a cost-effective architecture that supports most clients. Looking forward, however, advances in technology will limit the success of the current architecture and systems. Limiting pressures forcing software evolution already exist and are expected to continue to increase for the foreseeable future. Therefore, getting answer(s) to the question, "How do we accommodate these pressures and still grow our business?", becomes a very pressing issue.

There are a wide range of factors in play, both technical and financial, that will determine the path of future asset and infrastructure data management software: perceived and actual value, cyber security, advancements in assets themselves, and evolution of data transmission and communication systems – among many others. It is difficult to identify and prioritize all influencing factors, but it is possible to sketch a strategic overview of factors likely to impact the development process if we look to sequential patterns of data management systems evolution and integration.

In the 1990s, Supervisory Control and Data Acquisition (SCADA) systems were a leading-edge technology used to manage sensor-generated data and direct assets to accommodate changes defined by collected data using pre-programmed responses. SCADA promised substantial increases in productivity and equipment performance over manual operations. Proprietary, closed-architecture SCADA software, characterized by a process control focus and guarded by passwords and special programming, evolved into open architecture software. Protecting against competitors evolved into protecting against even more malicious cyber-attacks using ever larger "password" keys. But asset maintenance and management were barely considered in this advancement and seemed to lag in importance. SCADA systems were too specialized to organize and generate reports that would allow an asset to be operated and maintained – and SCADA could not accommodate the need for asset financial management functions. The 2000s signaled the emergence of dedicated computerized maintenance management system (CMMS) software. These programs gained market traction starting in large scale applications, such as cities and counties, and evolved to

accommodate smaller facilities through development of condensed function off-the-shelf applications. CMMS programs evolved because of an increasing awareness of the value of data. As the awareness of the data value continued to grow, a further need was generated for even more specialized asset management software to accommodate increasingly specialized (and presumed valuable) data sets. Yet despite this enhanced perception of data value, data security systems continued to take a secondary role to functions that could monetize data.

Now, in the year 2020, specialized asset management software, separate and apart from control and maintenance functions, has progressively raised its profile in response to increasing awareness of data value and the potential to exploit this value. [*In this discussion, the acronym, Asset Information Management System (AIMS), will be used to designate specialized asset management and data valuation software.*] The defining characteristic of all AIMS is the ability to project future events based on the monetized value of asset performance data, and the replacement value of the physical assets. Although the focus of AIMS is asset value management, it frequently accommodates varying degrees of hybrid functionality through integration with CMMS and, to a lesser degree, SCADA systems. A few AIMS have pursued more holistic capability. But few AIMS provide integral advanced data security functionality, instead choosing to focus on a core data management function. This focus on data management may be counterproductive if an advanced security dimension is not integrated into software at a level beyond that of simple password protection or prime number cryptography based Secure Socket Layer (SSL)/Transport Layer Security (TLS). Many current security systems still rely largely on this RSA type security, especially in small- to mid-size applications. However, in addition to SCADA, the 1990s produced Shor's algorithm and quantum computing. Shor's algorithm substantially weakened prime number-based RSA cryptography by accelerating the rate that prime number integers can be factored – effectively transforming "password" SSL/TLS based security from a robust firewall into a relatively weak deterrent. The perceived value of asset-derived data is poorly reflected in the capability provided by these security software systems.

AIMS cannot effectively monetize performance data without accurate and efficient data transmission, both between and among assets and users. 5G cellular has been touted as both the communications system and a business catalyst that will make accurate and efficient high-speed, high-volume data transmission a reality. But the benefits of greater speed, increased reliability, and transmission of greater volumes of data can be overshadowed by risk and liability. Clearly, with the proposed level of connectivity in a 5G system, a single data breach could potentially impact a very large number of organizations, very quickly, at potentially critical levels. Governments and multinational organizations, both foreign and domestic, have recognized this potentially fatal flaw in high-speed, high-volume data systems from both a defensive, as well as offensive, perspective. They are addressing cyber security both as a matter of national security and, as the definition of national security becomes increasingly blurred, as a matter of commerce. The majority of utility provider systems by number, especially smaller systems, continue to rely on SSL- and TLS-based security protocol. They remain vulnerable because they both support and are a part of commerce. As a result, smaller systems can provide a portal that allows unauthorized access not only to

their own data but also — potentially — the information of larger systems with more robust security. Considering the increasingly frequent occurrence of large-scale data breaches bannered by news feeds, the implementation of 5G protocol may magnify this already troubling condition and further spotlight the cost of data loss or compromise by not only financial services sectors, but in utilities sector as well. It is possible that organizations, including utilities, without a well-considered, integrated, multidimensional data management and security system will see vulnerability expand as AIMS and 5G become the standard of performance.

The promising potential of specialized AIMS and 5G connectivity cannot support the perceived value of asset and infrastructure data and data management capabilities without commensurate security capability. If asset management data truly provides value to owners, operators, maintainers, and managers, this data must be protected by an advanced cyber security system with capability proportionate to value. Quantum computing, until recently considered too theoretical for practical application, will be the basis for such capability. The direct integration of quantum computing functionality into both data management systems and connectivity must be the next collective evolutionary step in effective asset management. It should be initiated by replacement of RSA-derived systems with quantum key distribution (QKD)-based security systems. It may be a reasonable bet that quantum entanglement will be the successor to 5G connectivity as much as QKD will be the basis for the much needed next generation cyber security system. It will be interesting to see how the valuation of AIMS and 5G changes as quantum computing technology achieves second-generation development over the next five years.

Ironically, 20 ago, in 1998, the work of French Physicist Alain Aspect establishing the validity of quantum mechanics was confirmed – the same period that saw SCADA established as a leading-edge technology.